IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

La ciberradicalización: una nueva forma de victimización

Maria del Carme Guirao Cid
Universitat de Lleida

Fecha de presentación: septiembre de 2018
Fecha de aceptación: enero de 2019
Fecha de publicación: marzo de 2019

Resumen

Los atentados del 11-S significaron un antes y un después a la hora de entender el terrorismo. Por primera vez, una organización terrorista de base religiosa no solo atentaba contra un país occidental, sino que también utilizaba en beneficio propio las ventajas que proporcionaban las tecnologías de la información y la comunicación (TIC) para cometerlo. Desde entonces, el *jihad* pasó de ser un fenómeno local a adquirir una identidad global. Las organizaciones de este nuevo tipo de terrorismo (Al-Qaeda o Dâesh) nutren sus filas con individuos que han sido objeto de un proceso de adoctrinamiento y radicalización. Si bien al inicio este se realizaba exclusivamente en un entorno físico (*offline*), actualmente se observa como el ciberespacio (*online*) se ha convertido en el medio idóneo. En el caso de España, hace unos años el 80% de este proceso se producía en modalidad *offline* (mezquitas o centros universitarios), y siempre con la presencia de un agente radicalizador, pero tras la consolidación de las TIC, este porcentaje ha sido reemplazado por el entorno *online*. El presente artículo persigue un doble objetivo. El primero es ofrecer una explicación criminológica y victimológica al papel que tienen las TIC en el proceso de captación y radicalización *jihadista*. El segundo es realizar una comparación entre el proceso de adoctrinamiento *offline* y *online*.

Palabras claves

cibervictimización, *ciberjihad*, TIC, desinhibición, radicalización violenta, globalización

Tema

criminología, psicología, nuevas tecnologías

Cyber-radicalization: a new form of victimization

Abstract

The September 11th attacks marked a turning point in terms of our understanding of terrorism. For the first time, a religion-based terrorist organization not only attacked a Western country but also used the advantages of information and communication technologies (ICT) for its own benefit to carry out these attacks. From that point onwards, the jihad went from being a local phenomenon to acquire a global identity. The organizations operating within this new type of terrorism (Al-Qaeda or Dâesh) fill their ranks with individuals who have undergone a process of indoctrination and radicalization. While this initially took place in a physical setting (offline), nowadays, it is clear that cyberspace (online) has become the ideal medium. In the case of Spain, a few years ago, 80% of this process was conducted offline (in mosques or university centres) and always in the presence of a radicalizing agent. However, with the consolidation of ICTs, this percentage has been replaced by the online environment. This article has a dual objective. Firstly, it aims to provide a criminological and victimological explanation of the role of ICTs in the jihadist recruitment and radicalization. Secondly, it makes a comparison between the offline and online indoctrination processes.

Palabras claves

cyber-victimization, cyber-jihad, ICT, disinhibition, violent radicalization, globalization

Topic

criminology, psychology, new technologies

Introducción

La globalización[1] ha permitido desarrollar las tecnologías de la información y la comunicación (TIC[2]), ampliando los medios a través de los cuales las personas pueden interaccionar y comunicarse independientemente de la distancia geográfica que las separa.

En la actualidad, las TIC son algo más que un medio de comunicación, hasta llegar al punto de redefinir el modelo organizacional de las sociedades[3] y capacitar al ser humano con nuevas formas de pensar, aprender, actuar, representar y/o transformar la realidad. No obstante, el ciberespacio también se ha convertido en un medio para llevar a cabo conductas criminales: el ciberdelito. Según Wall (2007), este se puede definir como «cualquier comportamiento delictivo realizado en el ciberespacio».[4] El ciberdelito no ha conllevado la desaparición del delito tradicional, sino un cambio en la manera de realizarlo. Las TIC han generado nuevas oportunidades para la comisión de delitos, la creación de objetos más atractivos y accesibles, nuevos métodos de protección dirigidos a prevenir la cibervictimización, etc. (Turvey, 2012). Todo ello ha contribuido a extender la victimización más allá del ámbito físico.

Un ejemplo de todo ello lo tenemos en el uso que hacen las organizaciones terroristas de las TIC. Como veremos a continuación, la ventaja más visible del ciberespacio para

1. Ha sido definida como «un macroproceso histórico caracterizado por la sucesión de una compleja serie de procesos, conectados y convergentes, que han conllevado una aceleración de los cambios vitales y que están reestructurando radicalmente nuestras formas de vida. Expresándose en términos de una conectividad compleja, dialéctica y crecientemente intensificada, en la organización espacio-temporal de las relaciones sociales» (Giddens, 2001).
2. En esta tesis, el término *TIC* se usará como sinónimo de *Internet*.
3. Para mayor información, ver M. Castells, M. (2006).
4. Aunque el término *ciberdelito* es el más empleado, también es habitual que se haga referencia a este término como: *virtualcrime*, *onlinecrime*, *high-techcrime* o *digitalcrime*, entre otros.

las organizaciones es la mayor posibilidad de extender la ideología y narrativa *jihadista* más allá de los límites geográficos. No obstante, su uso también ha permitido alcanzar otros objetivos menos visibles, pero que repercuten de forma directa en el modo en que se van a perpetrar los atentados. Nos referimos a un mayor intercambio de información entre individuos, a tareas de planificación y coordinación, a difusión de propaganda en la que se ensalza y legitima el *jihad*, a desarrollar sistema de encriptación y a conseguir financiación y/o acceder al mercado de las armas. Incluso se ha observado que los grupos utilizan la herramienta Google Earth para conocer la situación geográfica y/o rutas de desplazamiento de algunos de sus objetivos (Tamimi, 2007; Cohen-Almagor, 2017). A todo este conjunto de prácticas, se les ha denominado «ciberterrorismo» (Cano, 2008).

1. Objetivos

El presente artículo persigue un doble objetivo.

El primero consiste en ofrecer una explicación criminológica, y en particular victimológica, sobre el adoctrinamiento *online* (o ciberradicalización), poniendo especial énfasis en las teorías de la oportunidad y de las actividades rutinarias.

El segundo consiste en describir las diferencias que se observan en los procesos de captación, reclutamiento y adoctrinamiento *jihadista* en su modalidad *online* respecto a la *offline*, así como conocer qué implicaciones que pueden conllevar estas en la estimación del riesgo de victimización real de un individuo.

2. Metodología

El artículo ha sido elaborado a partir de una revisión bibliográfica de artículos que han tratado el adoctrinamiento *jihadista* en modalidad *offline* y/o *online*.

La búsqueda se realizó a través de hemerotecas y en diferentes bases de datos, tanto a nivel nacional como internacional, con el objetivo de cubrir el mayor número de áreas temáticas.

A nivel internacional, fueron consultadas las siguientes bases de datos: SAGE Journals, ProQuest y Taylor and Francis Online, y Global terrorism databaseⅡ (GTD). En referencia a las hemerotecas, la búsqueda se realizó en: *Criminal Justice, Crime and Delinquency, Journal of Policing, Intelligence and Counter Terrorism, Studies in Conflict and Terrorism, The Crime Report, Criminal Justice Journalists, Journal of Terrorism Research y Perspectives on Terrorism*.

Los conceptos clave introducidos en los respectivos buscadores fueron: «cibervictimizacion», «Cyber jihad», «terrorism», «Jihadism and social networks», «Internet and Jihadism», «violent radicalization».

A nivel español, las fuentes consultadas fueron: Scientific Electronic Library Online España (SciELO), Dialnet, *Revista Española de Investigación Criminológica* (REIC), *Boletín Criminológico*, *Revista Electrónica de Ciencia Penal y Criminológica*, el Real Instituto ElCano, el Observatorio para la Prevención de la Radicalización Violenta (OPRA) y los documentos del Grupo de Estudios en Seguridad Internacional de la Universidad de Granada (GESI).

En este caso, los conceptos clave empleados fueron: «ciberterrorismo», «*ciberjihad*», «*jihad* y TIC», «adoctrinamiento», «ciberradicalización».

De acuerdo con los objetivos planteados, los criterios seguidos para incluir un estudio en la muestra fueron: (1) resultados publicados entre enero de 2000 y noviembre de 2018; (2) estudios originales en los que se analiza el proceso de adoctrinamiento y radicalización en el terrorismo de base religioso en su modalidad *offline*; (3) estudios originales en los que se analiza el proceso de adoctrinamiento y radicalización en el terrorismo de base religioso en su modalidad *online*; (4) estudios criminológicos que analizan el proceso a través de factores victimógenos; (5) estudios originales en los que se analiza el proceso de la ciberradicalización desde las teorías de la oportunidad y de los estilo de vida.

En total se han consultado treinta y tres estudios empíricos y/o teóricos.

3. Terrorismo y TIC

3.1. Factores victimógenos[5] en el ciberterrorismo

La conducta humana se muestra inconsistente cuando la persona deja de actuar en el espacio físico. En el caso del ciberdelito, esta disonancia está motivada por la protección y el anonimato (aparente) que ofrece la pantalla[6] y que hace del ser humano un individuo más valiente, mostrando mayor osadía a la hora de manifestar opiniones y/o emociones que de forma *offline* no se atrevería (Joinson, 2001). Este fenómeno fue definido por Suler (2004) como *the online disinhibition effect*[7] y diferenció entre aquel cuyos efectos eran positivos (*benign disinhibition*) de aquellos que causaban un daño (*toxic disinhibition*). Por ejemplo, en conductas como el *ciberbullying* o el *sexting*.

A nivel victimológico, este hecho dificulta la estimación del nivel de riesgo real que puede presentar un sujeto a convertirse víctima. Tomemos como ejemplo a un sujeto que en su día a día se muestra afable y educado con sus familiares y/o conocidos, en el colegio rinde adecuadamente, no protagoniza peleas, no muestra interés por la religión y/o por conocer la rama más radical del islam, entre otras cosas, pero en el muro de sus redes sociales observamos imágenes que denotan simpatía por una organización terrorista, realiza llamadas al *jihad* y/o justifica la matanza de «infieles».[8] Si desconociéramos su actividad en la red, el perfil de este sujeto debería ser considerado de «bajo riesgo», cuando en realidad su ciberconducta define un claro ejemplo de perfil de «alto riesgo» a ser víctima de un delito de captación y radicalización. No obstante, hay autores como Turvey (2012) que discrepan del efecto de la desinhibición *online* y defiende que, si bien la persona puede actuar de forma diferente a como lo haría en la vida real, toda actividad realizada en el ciberespacio siempre guarda similitud con el patrón de conducta no virtual del sujeto.

Para entender por qué se produce esta desinhibición que nos convierte en seres más vulnerables al ciberdelito, debemos atender a cada uno de los cinco elementos que Suler (2004), y posteriormente Agustina (2014), corroboraron como generadores de oportunidades delictivas:

1. Anonimato disociativo (*You don't know me*): se erige como el efecto principal de la desinhibición al ser el responsable de que podamos navegar por la red, pudiendo cometer delitos sin temor a ser descubiertos. Las características de las arquitecturas digitales han complicado la tarea de los cuerpos de seguridad en materia de prevención e identificación de los victimarios[9] al dotar a estos últimos de un conjunto de mecanismos que les garantiza el anonimato. Por ejemplo, pudiendo utilizar nombres de usuarios o direcciones de correo electrónico que nada tienen que ver con sus nombres de pila.

Otra consecuencia directa que deriva del anonimato disociativo reside en la posibilidad que se da al individuo de separar su *yo* real del *yo* digital, permitiéndole de esta manera actuar a través de una representación de él mismo. Esto hace que el individuo estructure un segundo *yo* que no tiene por qué ser único, sino que, fruto de las características que presenta la red, se le permite elaborar más de uno, lo que desencadena identidades múltiples (Becoña, 2016)

2. Invisibilidad (*You can't see me*): este factor actúa en una doble dirección. Por un lado, permite al sujeto actuar sabiendo que la autoría de la conducta difícilmente le va a ser atribuida. Y, por otro lado, sabe que puede visualizar contenidos privados de otros individuos sin que estos lo sepan.

3. Comunicación asincrónica (*See you later*): si bien las TIC han permitido eliminar las variables espacio y tiempo de la comunicación interpersonal, ello no garantiza que esta vaya a producirse de forma inmediata. Puede que la pregunta lanzada por el emisor no sea contestada hasta pasado un lapso temporal, que puede ir desde escasos minutos a horas o incluso días. Por lo tanto, con las TIC

5. Los «factores victimógenos» son un concepto utilizado en la victimología para hacer referencia a aquellos factores cuya presencia permite estimar el riesgo de victimización que puede sufrir una persona.
6. José Agustina lo denomina «máscara virtual».
7. «El efecto de la desinhibición *online*».
8. Moussa Oukabir, uno de los integrantes de la célula terrorista de Ripoll, publicó en su perfil en Kiwi: «Mataría a todos los infieles, solo dejaría a los musulmanes que siguiesen la religión» o «La muerte es segura, la vida no».
9. Según la teoría de las actividades cotidianas (Cohen Felson, 1979), podríamos decir que los *Guardianes capaces* caen de la tríada del crimen.

la respuesta inmediata del receptor deja de ser obligada, generando un halo de misterio o suspense a aquel que espera la respuesta.

4. Introyección solipsista (*It's all in my head*): la ausencia de interacción física favorece la consolidación de lazos y la desindividualización del sujeto a favor de una identidad grupal. Cuando recibe un mensaje o lee una aportación en un foro, la persona percibe esta información como la «única» existente y veraz. A partir de ese momento, toda información que proviene de una fuente externa al endogrupo es puesta en duda.

5. Minimización del estatus y la autoridad (*Your rules don't apply here*): en el mundo *offline*, la autoridad y el poder son dos de las cualidades que describen a un tipo determinado de persona. En el ciberespacio, el peso que tienen estos dos elementos se reduce, haciendo que cualquier persona tenga las mismas oportunidades de hacerse con ellos. De hecho, la máxima de internet es «todo el mundo es igual en la red. Todo el mundo puede compartir sus opiniones libremente con los demás» (Suler, 2004).

En el ciberterrorismo, la suma de todos estos factores victimógenos contribuye a disminuir el umbral de riesgo percibido por el sujeto, y a aumentar las probabilidades de que este acabe cometiendo el delito (convirtiéndose así en cibervictimario), o sea, seducido por narrativas extremistas que pueden llegar a generar en él o ella estados de dependencia (convirtiéndose así en cibervíctima).

El desinhibidor «digital» encuentra su homólogo *offline* en el consumo de bebidas alcohólicas o sustancias tóxicas en los momentos previos a la comisión del atentado. Por ejemplo, nos referimos al consumo de captagón[10] (también conocida como la «droga de los *jihadistas*»). Esta es una droga que empezó a producirse con finalidades terapéuticas para cuadros clínicos de hiperactividad, narcolepsia o depresión. No obstante, el efecto que producía era similar al de las anfetaminas. Es decir, generaba un estado de hipervigilancia, ausencia de hambre, y disminución del cansancio, del dolor y de la empatía. Estos efectos hicieron que se descartara. No obstante, las organizaciones terroristas han sabido darle un nuevo uso. Actualmente se la conoce como la «droga de los *jihadistas*», al ser consumida por parte de combatientes sirios en combate o por haberse hallado en algunos de los escenarios previos a la materialización de atentados en suelo europeo. Por ejemplo, en los domicilios de los responsables de la oleado de atentados de París en noviembre de 2015.[11]

3.2. El uso de las TIC por parte de los grupos terroristas

3.2.1. Las TIC como productor y difusor de la narrativa *jihadista*

La primera organización terrorista de base religiosa que usó las TIC como herramienta para la difusión de la ideología y narrativa *jihadista* fue Al-Qaeda a través del sistema VHS, con la creación de su propia productora, Al-Andalus, y la publicación de su propia revista, denominada *Inspire*. De esta manera, la organización no solo desposee de toda capacidad crítica a los medios autóctonos, sino que también los subordina a la ideología *jihadista* (Cohen-Almagor, 2017). Desde entonces son cada vez más las organizaciones terroristas que han encontrado en las TIC la solución a muchos de los problemas que tenían a la hora de extender su ideología.

A partir de 2014, coincidiendo con la autoproclamación del *proto* Estado Islámico, los recursos económicos que destinan las organizaciones a tareas propagandísticas no paran de crecer, dado que el objetivo final es elaborar contenidos de alta calidad, hasta el punto de compararse con producciones hollywoodenses. Esta realidad no es ajena a España. Según un estudio realizado por Reinares y García-Calvo (2017), entre 2013 y 2017, el 59,7 % de las tareas que han realizado las células terroristas operativas dentro de las fronteras españolas respondían a tareas de enaltecimiento y difusión de propaganda.

Otro de los objetivos que busca el grupo terrorista con la gestión de sus medios de comunicación es conseguir la máxima atención mediática internacional posible, así como difundir a nivel planetario su cosmovisión apocalíp-

10. El captagón es una droga muy populare en Oriente Próximo y Oriente Medio, sobre todo en Siria.
11. Al respecto puede leerse una noticia publicada en el diario *El Mundo* en noviembre de 2015: <https://www.elmundo.es/internacional/2015/11/19/564ce223ca474114118b45af.html>.

tica, para conseguir generar un efecto movilizador entre sus simpatizantes (Carbonell, Torres y Fuster 2016). Para ello, la organización no solo se presenta como «víctima» de una teoría conspiratoria que quiere humillar y oprimir al islam, sino también como un ente superior respecto a su «enemigo».

Para elaborar el contenido de la propaganda *jihadista*, las organizaciones acuden a dos fuentes. La primera responde al fenómeno *fanboy* o *fangirl* (Conway, 2016). Se trata de individuos jóvenes, con dominio del entorno red y que se encuentran atravesando una crisis de identidad, presentan problemas de arraigo y/o están afrontando un desafío intercultural, los cualesencuentran en el entorno TIC la vía para poder conseguir el reconocimiento y protagonismo que según ellos el entorno *offline* les priva, al ser un medio que permite reducir la sensación de aislamiento (Waldmann, 2010). El solo hecho de acceder a un tipo de contenido que saben que también es visionado por otras personas hace que aflore en él o ella la sensación de formar parte de una gran comunidad. A su vez, esta refuerza el vínculo con los elementos identitarios del grupo, lo que puede crear dependencia. No obstante, los *fanboy* o *fangirl* son individuos que no guardan relación formal con la organización terrorista, solo se dedican de manera voluntaria a la elaboración o redifusión de material propagandístico *jihadista* a través de sus perfiles en redes sociales,[12] contribuyendo con su conducta a generar un efecto multiplicador (Miró, 2011). De esta manera, podemos decir que el fenómeno *fanboy o fangirl* permite elaborar la propaganda a través de un proceso *bottom-up*.

Sin embargo, todas estas características también pueden actuar como factores victimógenos y convertir a estos individuos en objetivos apropiados y apetecibles para los ciberterroristas,[13] aun sin ser ellos plenamente conscientes del riesgo que pueden conllevar las conductas que realizan tras la pantalla.

La segunda fuente para la elaboración propagandística responde al de un individuo (hombre o mujer[14]) que sí forma parte de la organización terrorista y que, como consecuencia de su elevado conocimiento en el manejo de las TIC y los programas audiovisuales, le son asignadas tareas de elaboración y difusión de propaganda *jihadista*. Para que esta resulte atractiva a futuros reclutas, estos individuos introducen elementos racionales, emocionales y cognitivos (Jordán, 2009). Con el objetivo de llegar al mayor número de receptores, su contenido es publicado en diferentes idiomas, de los cuales los más habituales son diferentes dialectos del árabe, inglés, francés y español.

Independientemente de la fuente a partir de la cual elaboran su propaganda, ambos perfiles representan el claro ejemplo del concepto de «prosumidor» que McLuhan y Nevitt (1972) y Toffler (1980) definieron para hacer referencia a aquel individuo que no solo visiona y consulta contenido en la red global, sino que contribuye a su creación.

3.2.2. La influencia de la narrativa *jihadista online* en el receptor

Han sido varias las teorías elaboradas con el objetivo de conocer los efectos que el mensaje propagandístico

12. Conviene recordar que la exposición voluntaria a este tipo de material puede iniciar en el sujeto un proceso de autoadoctrinamiento y facilitar así su cibervictimización. Desde la última reforma del Código penal de 2015 en materia de terrorismo, la conducta de autoadoctrinamiento pasó a ser castigada con penas de prisión que oscilan de los dos a los cinco años, de acuerdo con el contenido del artículo 575.2. Según el mismo: «Se entenderá que comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines. [...] Asimismo, se entenderá que comete este delito quien, con la misma finalidad, adquiera o tenga en su poder documentos que estén dirigidos o, por su contenido, resulten idóneos para incitar a la incorporación a una organización o grupo terrorista o a colaborar con cualquiera de ellos o en sus fines». Esto significa que, por primera vez, el legislador considera las TIC como un elemento clave para la materialización de delitos terroristas, al encontrar los grupos terroristas en ellas el marco perfecto en el cual poder exponer, difundir y justificar su ideología, así como planificar la logística de los atentados. Reproduciendo palabras de la actual ministra de Justicia, Dolores Delgado (antigua Fiscal coordinadora contra el terrorismo yihadista en la Audiencia Nacional): «A través de internet, el yihadismo se ha convertido en un terrorismo global» o «El yihadismo es un terrorismo mutante».
13. Desde la teoría de las actividades cotidianas (TAC) de Cohen y Felson (1979) hubieran sido considerados *suitables targets*.
14. De acuerdo con el estudio de Reinares y García-Calvo (2017), se observa una dimensión de género que tiende a perpetuar los roles que operan en la sociedad. De este modo, observamos que mientras los hombres se dedican mayoritariamente a tareas de radicalización y reclutamiento (83,5 %) y enaltecimiento y difusión propagandística (57,1 %), a ellas se les encomienda además el traslado de personas a zona conflictiva (76,2 %).

puede tener en el receptor. A continuación se exponen las más representativas y se relacionan con la narrativa *jihadista*.

a) Teoría del impacto directo (Katz y Lazarsfeld, 1995). Parte de principios mecanicistas para defender que los mensajes emitidos por parte de los medios pueden, por sí solos, provocar sobre el receptor la respuesta deseada.

Esta teoría explica la necesidad que manifiestan organizaciones terroristas como Dâesh de alcanzar la máxima calidad en cada una de sus producciones. Para ello cuidan planos, secuencias, iluminación, gestualidad, vestimenta, etc. o introducen efectos especiales y *nasheeds*.[15] Todo ello con el objetivo de que su estética se asemeje a la de los videojuegos o, como ya se ha mencionado, a las películas de Hollywood. Si bien han sido diversas las filmaciones que las organizaciones han hecho públicas, puede que los que mayor impacto emocional han provocado fueron la decapitación del fotoperiodista James Wright Foley (1973-2014) y el asesinato del piloto jordano Muad al Kasaesbe (1988-2015) tras quemarlo vivo encerrado en una jaula vistiendo un mono naranja de preso, recordando la estética característica del centro de detención de Guantánamo.

b) Teoría del doble flujo de comunicación (Katz y Lazarsfeld, 1995). Defiende que el poder de los medios como generadores de respuestas inmediatas es limitado. Para conseguir sus objetivos, no basta con difundir un mensaje que impacte directamente sobre un destinatario, sino que también ha de haber otro individuo físico que transmita la misma información.

Esta teoría recoge la importancia que tienen las relaciones de un sujeto con su grupo de iguales o familiares (Jordan, 2009; Toboso, 2013). Este hecho queda manifiesto al analizar el proceso de captación, reclutamiento y radicalización que atravesaron algunos de los autores de atentados terroristas cometidos en suelo europeo. Son ejemplo los hermanos Kouachi (autores del atentado contra la sede de Charlie Hebdo en 2015); el grupo de Abdeslam (implicados en los atentados de la noche del 13 de noviembre de 2015 en París); los hermanos El Bakraoui (autores del atentado en Bruselas ese mismo año); los hermanos El Jelay (cuatro marroquíes detenidos en una operación anti terrorista en Girona y acusados de financiación a la organización terrorista Dâesh[16]), o la relación de amistad y/o parentesco que guardaban la mayoría de los integrantes de la célula de los atentados de Barcelona y Cambrils.

c) Teoría de los usos y gratificaciones (Katz, Blumer y Gurevitch, 1973). A diferencia de las anteriores, esta defiende que el efecto no viene dado por el medio, sino que es el propio consumidor quien lo genera. Es decir, el receptor deja de ser un agente pasivo para convertirse en un ser activo, al ser él o ella quien interacciona e interpreta el contenido propagandístico que recibe.

Por otro lado, esta capacidad repercute en los medios generadores del mensaje, pues se ven obligados a competir entre ellos para satisfacer las necesidades de la audiencia y conseguir que estos los elijan como fuente de información. Esta teoría explicaría la pugna que se observa entre organizaciones terroristas para hacerse con el monopolio propagandístico en la red; de hecho, se podría decir que la rivalidad *offline* entre organizaciones terroristas se ha generalizado al mundo *online*.

3.2.3. Las TIC como medio de captación, reclutamiento y radicalización

Desde la comisión de los atentados a las Torres Gemelas y al Pentágono el 11 de setiembre de 2001 en Estados Unidos (conocido como 11-S), se ha tenido constancia de procesos de adoctrinamiento *jihadista*. Los primeros se llevaron a cabo en el entorno *offline*, pero con la emergencia de las TIC se trasladaron, también, al entorno *online*. Esta modalidad supone que el proceso puede llevarse a cabo exclusivamente vía internet, sin mediar interacción física entre los agentes implicados. No obstante, el estudio de Vicente (2018) nos muestra que todavía son muy pocos (uno de cada diez) los casos en los que un sujeto ha podido alcanzar el estadio de la radicalización solo mediante la red.

15. Un *nasheed* es un canto a capela de temática religiosa que realizan los seguidores del credo mahometano. Las organizaciones terroristas los utilizan para publicitar sus acciones y conseguir reclutar a nuevos miembros.
16. Su detención fue la primera en la que todos sus miembros formaban parte de una misma familia.

Los primeros en alertar del uso de las TIC con finalidades de radicalización terrorista fueron Sageman (2004) y Weimann (2004). Desde entonces se ha constatado que cada vez son más las personas que deciden unirse al *jihad* después de haber tenido un primer contacto con la ideología por internet. Esta conducta se observa especialmente en el colectivo de jóvenes, dado que es la primera generación que ha crecido con las TIC (Cohen-Almagor, 2017). La bibliografía los ha definido como «nativos digitales» (Prensky, 2001) y se caracterizan por ser individuos que reciben rápidamente la información, les gusta estar haciendo distintas cosas a la vez, prefieren la imagen al texto, el acceso aleatorio, funcionan mejor cuando trabajan en red, realizan sus tareas pensando que se trata de un juego, y su eficacia y productividad aumenta cuando son sometidos a un sistema de recompensa continua. Todo ello les hace ser individuos con dificultades para diferenciar sus acciones del ámbito analógico respecto al digital. No obstante, un menor conocimiento de la red no significa restar al margen de la influencia *jihadista*. Las generaciones anteriores, aun sin haber crecido en un mundo digital, se han acercado a esta tecnología y han aprendido su funcionamiento. Son «inmigrantes digitales».

En España, las instituciones no prestaron interés a esta realidad hasta 2011 a raíz de la publicación de la Circular 2/2011 por parte de la Fiscalía General del Estado.[17] Posteriormente, en 2015, el Ministerio del Interior hizo público un informe en el que manifestaba que en España el 80 % de la captación y el adoctrinamiento se producía en lugares físicos, como eran las mezquitas o los centros universitarios, y con la presencia siempre de un agente radicalizador físico. Este se caracteriza por ser una persona carismática, con un poder de seducción elevado sobre los demás, y con dotes para el liderazgo.

En la actualidad, este predominio ha sido reemplazado por internet, hasta el punto de convertirse en el centro virtual del islamismo radical y del *jihad* (Cano, 2008; Reinares y García-Calvo, 2017; Reinares, García-Calvo y Vicente, 2018). No obstante, el cambio de medio operacional no conllevó el olvido de la vía *offline*. En 2017, Reinares y Gracía-Calvo publicaron un estudio en el que analizaban el perfil de detenidos en España por actividades terroristas entre 2013 y 2016, y concluían que la radicalización se producía mayoritariamente en entornos mixtos (40,3 %), es decir, combinando la modalidad *offline* con la *online*. Más recientemente, los mismos autores, junto a Vicente (2018), han vuelto a corroborar el mayor uso de las TIC como medio adoctrinador, al concluir que del total de los individuos condenados o muertos por actividad terrorista en España entre 2012 y octubre de 2018, el 79 % fue radicalizado en el ciberespacio. Pero si se acotaba el límite temporal de 2013 a octubre de 2018, ese porcentaje se elevaba hasta el 92,1 %.

La preferencia por el uso de una modalidad u otra está condicionada por el grado de conocimiento que existe entre agente adoctrinador e individuo a adoctrinar. Según Vicente (2018), se observa que a mayor conocimiento entre ambos, el escenario preferente para la radicalización es el *offline,* donde un familiar o un amigo suele ser el agente radicalizador en la mayoría de los casos (Holman, 2016; Reinares y García-Calvo, 2017; Kruglanski, Webber, Cnernikova y Molinario, 2018), mientras que cuanto menor sea este, más importancia tiene la modalidad *online*, pues la pantalla es un elemento que permite al adoctrinador acercarse a un sujeto desconocido para intentar persuadirlo de que entre en la organización. Solo cuando el nivel de confianza entre los sujetos es el óptimo, el reclutador propone un primer encuentro «cara a cara», sin que ello signifique dejar de interactuar en el ciberespacio. A partir de ese momento, la radicalización se produce tanto en el entorno *offline* como en el *online*.

El mayor peso de las TIC en el proceso de radicalización explicaría, en parte, la reducción temporal que necesita un sujeto para alcanzar el estadio máximo de determinación hacia el acto *jihadista*, reduciéndose de años a solo unos meses. Este fenómeno se ha venido denominando, por parte de la prensa y algunos expertos, como «adoctrinamiento *express*». Por lo tanto, la ciberradicalización no es un proceso que haya aparecido paralelamente a la implantación de las TIC, sino que las organizaciones han sabido redefinirla hacia el ciberespacio para sacarle mayores beneficios (Grabosky, 2001).

17. Circular 2/2011 de la Fiscalia General del Estado sobre al reforma del Código penal por Ley orgánica 5/2010, en realción con las organizaciones y grupos criminales. Puede consultarse en: <https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/circular%202-11.pdf?idFile=7e10b69f-d6b8-4e02-980b-737045993138>.

3.2.3. Infraestructura para la captación y radicalización *online*

Para lograr la captación de nuevos miembros, las organizaciones se dotan de distintas infraestructuras, lo que permite que un único cibervictimario pueda incidir sobre diversos destinatarios a la vez. Las infraestructuras que más utilizan estas son:

a) Páginas web: las organizaciones disponen de sitios web a través de los cuales se dan a conocer y permitiendo al simpatizante descargarse todo tipo de materiales (vídeos, comunicados, *nasheeds,* etc.) que les permita empezar a interiorizar la ideología *jihadista*. Algunos ejemplos de webs: «AQ/QA», «Al-ansar» o «Muslims news». No obstante, a causa del auge de las redes sociales, estas han ido perdiendo fuerza. Las redes sociales son herramientas más difíciles de controlar y cerrar por parte de los cuerpos de seguridad. En caso de que así se produjera, el grupo puede abrir nuevos perfiles en cuestión de escasos minutos.

b) Perfiles en redes sociales: las redes sociales son consideradas la puerta de entrada a la organización, dado que son medios fáciles de activar, de acceso rápido y permiten publicar contenido de forma instantánea e ilimitada. Esto permite al sujeto estar informado a todas horas, así como interaccionar con otros individuos a través de las aplicaciones de chat de las que disponen estos programas. No obstante, se ha constatado que las redes sociales también son utilizadas con finalidades operativas, en el sentido de ser espacios donde las organizaciones compran armas y munición para sus acciones (Cohen-Almagor, 2017).

c) Foros y chats: el grupo sabe que es muy importante que su contenido esté actualizado, pues los foros y chats son considerados auténticas «cajas de resonancia» de la ideología *jihadista*. Para poder acceder a estos, el individuo ha de haber recibido antes unas claves. Esta restricción de acceso no solo añade un plus de dificultad a las operaciones antiterroristas, haciendo necesario recurrir a la infiltración de alguno de sus agentes para poder conocer el contenido de las conversaciones que ahí se mantienen, sino que también genera en el sujeto un sentimiento de «exclusividad», además de reforzar el sentido de pertenencia grupal a la organización, lo que da origen a fuertes lazos de amistad entre los individuos que acaba derivando en un microcosmo digital (Miró, 2011, 2013; Cohen-Almagor, 2017).

Por ello, no sería descabellado adaptar los perfiles de Kozinets (2010) a la dinámica de la organización terrorista. De este modo, encontraríamos: los «novatos» (*newbies*; individuos que han accedido a la comunidad de forma reciente y aún deben aprender el lenguaje cibernético usado por la organización); los «integradores» (*minglers;* individuos que ya pertenecen a la organización y se dedican a socializar y preservar los vínculos ya existentes en ella); los «devotos» (*devotees*; individuos que anteponen la actividad ciberterrorista a la tarea de preservar los vínculos de la comunidad), y los «enterados» (*insiders*; individuos que se comprometen tanto con la actividad de la organización como con la tarea de preservar los vínculos que la unen).

d) Videojuegos: esta herramienta permite trasladar situaciones socioculturales del mundo real al mundo virtual. La bibliografía ha hecho clasificaciones de estos atendiendo a distintas variables. No obstante, nos vamos a centrar en los videojuegos masivos (*Massively Multiplayer On-line role playing game*; MMORPG) de temática bélica, como *Call of Duty Black Ops* o *Gran Theft Auto*. Estos son los más utilizados por parte de las organizaciones terroristas a la hora de captar a futuros miembros, puesto que requieren poco desgaste mental por parte del jugador. Se ha observado que algunas organizaciones terroristas han elaborado sus propios videojuegos[18] o modificado los comerciales añadiendo opciones que los hagan más próximos al estilo *yihadista* (por ejemplo, ejecutar personas al grito *Allahu Akbar*, diseñar escenarios que reproducen las calles de Siria, introducir el traje naranja de los presos de Guantánamo, etc.).

Un ejemplo del uso de los videojuegos con finalidades terroristas, más allá de la captación y el reclutamiento, lo tenemos con el uso que hicieron de PlayStation 4 los integrantes de la célula que atentó en París en noviembre de 2015. Según las informaciones policiales, los miembros de la célula utilizaron los juegos en línea para planificar el recorrido y seleccionar los objetivos contra los cuales iban a atentar a lo largo de toda la noche, así como para

18. Por ejemplo, Hezbolá con *Special Force 2*.

comunicarse a través de la aplicación PlayStation Network de que dispone la máquina.[19]

Para jugar a un MMORPG, el sujeto debe interactuar con otros jugadores de forma simultánea, que al igual que él se encuentran conectados a la red (Carbonell, Torres y Fuster, 2016). Al ser un mundo no físico, el sujeto sabe que la violación de las normas del juego no le reportará un castigo «real». De este modo, las variables que describieron las teorías de la disuasión o preventivas como disuasivas de la comisión del delito (severidad, celeridad y certeza), aquí quedan neutralizadas. Esto aleja al jugador del coste real de su conducta.

Otro aspecto que caracteriza a este tipo de videojuegos es la alteración de la identidad. Si quiere jugar, el sujeto está obligado a crear un avatar antes de iniciar la partida. Este se define como el elemento gráfico que encarna o representa al sujeto real. No obstante, este no tiene que reproducir fielmente todas las características de la persona. De este modo, el sujeto puede proyectar en él su *yo* ideal, que puede darle mayor satisfacción que su *yo* real (Carbonell, Talarn, Beranuy y Oberst, 2009).

Ambos hechos contribuyen a que el sujeto se comporte de manera impulsiva, irreflexiva y desinhibida, dejando abierta la posibilidad de materializar sus fantasías en el mundo virtual.

Dado el número elevado de jugadores, los MMORPG permiten formar clanes o grupos de jugadores para jugar una partida. Los miembros del grupo comparten los mismos objetivos y son los responsables de definir la narrativa del juego y los roles que cada uno va a desarrollar en ella. Para ello, esta modalidad de videojuegos dispone de aplicaciones de mensajería instantánea (chats o mediante auriculares con micrófonos) que permiten a los sujetos conversar mientras juegan la partida, sabiendo que su contenido quedará en el ámbito de la privacidad y no será divulgado a terceros. Del mismo modo, al ser juegos *online*, la partida no se termina al cerrar la sesión del jugador, sino que el juego va evolucionando durante el período de tiempo en el cual el jugador no está conectado. Este hecho hace que la panificación de la partida por parte del grupo esté en constante redefinición, y que se genere un cierto estado de «obligatoriedad» de jugar si se quiere lograr un mayor control de la situación y vencer así a otros grupos de jugadores.

3.3. Fases del adoctrinamiento a través de las redes

En el terrorismo de base religiosa, el adoctrinamiento se define como aquel proceso a través del cual un individuo adopta actitudes y creencias que justifican, tanto utilitaria como moralmente, el terrorismo inspirado en una versión salafista, y tiene lugar tras la previa captación y reclutamiento por parte de una organización terrorista (Cano, 2008; Reinares y García-Calvo, 2017). Si de por sí el proceso es difícil de identificar, el fenómeno se torna mucho más complejo cuando el medio utilizado es la red.

El proceso de adoctrinamiento se estructura en cuatro fases, a través de las cuales se generan los tres elementos necesarios que, según la teoría de la búsqueda de la significancia (*Significance Quest Theory*, SQT), se requieren para que un individuo complete la fase de radicalización en una ideología extremista y decida dar el paso hacia la acción terrorista. Estos son: la necesidad, la narrativa y la red de apoyo (Kruglanski, Jasko y LaFree, 2016; Kruglanski, Webber, Cnernikova y Molinario, 2018). No obstante, como se verá a continuación, se aprecian diferencias según el medio a través del cual se desarrolle el proceso, es decir, vía *online* o vía *offline* (ver tabla 1).

a) Aproximación y primeros contactos: a diferencia de lo que sucede en la modalidad *offline,* esta fase puede producirse de dos maneras, según la mayor o menor iniciativa que muestra el sujeto en el reclutamiento. Para ello vamos a diferenciar entre «aproximación activa» y «aproximación pasiva».

En la primera (aproximación activa), es el propio individuo quien decide ponerse en contacto con la organización, aun sin ser consciente de las consecuencias que esta acción le puede acarrear. El individuo responde a un perfil de persona joven, que experimenta sentimientos de humillación, frustración, culpa, odio, ira y/o indignación, como respues-

19. Pueden verse noticias al respeto en *El Periódico* y en *As*: <https://www.elperiodico.com/es/internacional/20151115/terroristas-atentado-paris-emplean-playstation-para-comunicarse-4674944> y <https://as.com/meristation/2015/11/16/noticias/1447666620_150790.html>.

ta a experiencias personales y/o por hechos negativos que han sucedido en su entorno. Todos ellos actúan como *push* (precipitadores o potenciadores) para que el individuo tome la iniciativa de ingresar en un grupo. El sujeto se conecta a la red y empieza a buscar información *jihadista* sin que esta tenga que guardar relación directa con una organización terrorista o con contenidos que se muestren proclives a la violencia *jihadista*, pudiendo responder a la simple curiosidad del sujeto. De esta manera, estos sujetos podrían ser considerados como víctimas propicias pasivas a la cibervictimización terrorista (Cohen y Felson, 1979). Debemos recordar que en el ciberespacio la conducta decisional del sujeto se ve limitada por la ingenuidad y la impulsividad que conlleva actuar a través de internet (Agustina, 2014). Esto se debe al hecho de que los elementos que constituyen el entorno virtual actúan directamente en la vía emocional del sujeto (De la Corte, 2015; Bouzar, 2015, 2017). No obstante, conductas aparentemente «inocentes» como las descritas pueden ser interpretadas por el ciberreclutador como una «provocación» a la voluntad de entrar a formar parte de la organización.

Cuando la conducta del sujeto va más allá de la simple curiosidad, la búsqueda no se detiene; incrementa las horas frente al monitor y va profundizando en el contenido que alberga la red. Esta conducta de búsqueda «obsesiva» le permite interiorizar los postulados *jihadistas*. En este punto, el sujeto visita los perfiles que las organizaciones tienen activos en la red en cuentas como Facebook, Instagram, Twitter o Kiwi. Por ejemplo, con un solo clic puede observar y/o descargar imágenes de la guerra en Siria, ver cadáveres de mujeres y niños asesinados por el «enemigo», tratos vejatorios contra la comunidad musulmana, la respuesta pasiva de Occidente, etc. Estos materiales contribuyen a la elaboración de una narrativa victimista que es utilizada por la organización con un doble objetivo: para generar en el individuo el deseo de venganza y para justificar y legitimar el uso de la violencia (Trujillo, Moyano y González-Cabrera, 2006; Kruglanski, Webber, Cnernikova y Molinario, 2018). Por otro lado, la visualización de este tipo de materiales hace que el sujeto empiece a cuestionarse tanto su estilo de vida como el sistema de creencias en el cual ha sido socializado, para pasar a adoptar un pensamiento desindividualizado y dicotómico, a diferenciar entre un «nosotros» y un «ellos». De forma paralela, el sujeto experimenta sentimientos de rabia y odio hacia Occidente, y empatía y solidaridad hacia la comunidad musulmana (*Umma)*. Esto hace que cualquier conducta o comentario que se realiza sobre el pueblo musulmán, y que el sujeto interpreta como «injusto», «cruel» o «humillante», lo perciba como un ataque a su propio ser. Es lo que Khosrokhaver (2003) denominó «humillación delegada».[20]

Estas circunstancias hacen que el sujeto tome una nueva conciencia de su entorno y redefina su proyecto de vida de acuerdo a la ideología de la organización. Así se constató en los atentados contra Mohammed Bouyeri, terrorista que asesinó al director de cine Theo van Ghohg en noviembre de 2004. De ellos se desprende que el interés por el islam dejó paso al visionado de materiales extremistas, y de eso a frecuentar sitios web *jihadistas*.

En la segunda modalidad (aproximación pasiva), es una persona[21] de la organización la que se dedica a tareas de captación y reclutamiento *online*, quien inicia las conversaciones con el sujeto. El ciberadoctrinador se dedica a rastrear perfiles para localizar aquellos individuos que, atendiendo a la información que esté incorporada en sus muros, puede ser fácilmente reclutable para posteriormente adoctrinarlo. Por ejemplo, los responsables materiales de los atentados de Barcelona y Cambrils de agosto de 2017 habían colgado varias fotografías y vídeos en los perfiles de sus respectivas cuentas de redes sociales en las que se podía apreciar un perfil de sujetos jóvenes «buscadores de sensaciones», que les gusta el ocio, la velocidad y/o el riesgo.[22] Estos factores victimógenos personales son los que indican a los ciberojeadores que ese sujeto puede ser un «buen candidato» para la comisión de atentados suicidas. Todo ello nos lleva a tomar conciencia de que las TIC han favorecido la emergencia de una nueva relación entre nuestro cuerpo y la máquina, una nueva subjetividad digital.

20. Este sentimiento va a alcanzar su máximo en la cuarta fase del proceso: fase de yihadización.
21. Si siguiéramos la teoría de las actividades rutinarias aplicada la cibercriminalidad de Miró Linares (2011), lo podríamos definir como «el ciberagresor motivado».
22. Puede verse la siguiente noticia, publicada en el diario *El Mundo:* <https://www.elmundo.es/cronica/2017/09/05/59aa847ae5fdea963d8b4621.html>.

b) Captación, adhesión y prerradicalización: una vez sujeto y ciberreclutador han establecido los primeros contactos, las conversaciones se trasladan a foros y/o chats privados en los cuales el individuo percibe que ya forma parte de la *Umma* virtual. Previamente el sujeto recibe las claves de acceso y se descarga el software TOR[23] en su ordenador para evitar que su navegación deje huella (*cybertrails*) susceptible de ser rastreada por parte de agentes policiales.

Una vez el individuo pasa a formar parte del grupo (o cibercomunidad), desea satisfacer una nueva necesidad: la de significación social. El sujeto necesita ser reconocido y respetado por su grupo (Bandura, 2004; Baumeister y Jones, 1978; Baumeister y Leary, 2017). Ello hace que toda información trasnmitida dentro del grupo sea reinterpretada de acuerdo con su sistema de creencias y valores. Esta dinámica favorece la consolidación del compromiso de los miembros con la organización y promueve la narrativa radical al estar todos involucrados en un proceso de aprendizaje colectivo, donde la retroalimentación es constante (Kruglanski, Jasko, Webber y Cnernikova, 2018). Cuando este suceso tiene lugar, significa que el sujeto ya ha iniciado el camino que le va a llevar a aceptar un encuentro «cara a cara» con un miembro de la organización.

La restricción que caracteriza esta fase se debe al grado de extremismo violento que toman las conversaciones. Se recurre a los suras del Corán donde abundan las referencias al *jihad*, al martirio, y a la promesa de la glorificación y el acceso al Paraíso del individuo, y de sus familiares, una vez haya muerto matando. De este modo se convence, mediante la manipulación, la mentira y/o el engaño, al sujeto para que cometa un hecho delictivo. Del mismo modo, para justificar el uso de la violencia, la organización le enseña a apelar a la mayor lealtad de Alá, a la condena de los condenadores o a la negación de la víctima, que se corresponde con las técnicas de neutralización descritas por Sykes y Matza[24] (1971).

Además de este tipo de información, el miembro de la organización usa todo tipo de habilidades comunicacionales para aproximarse al sujeto, ganarse su confianza y facilitar así el encuentro en la vida real.[25] Para ello, el ciberreclutador querrá conocer sus vulnerabilidades, su estilo de vida, sus problemas familiares, su estatus socio-económico, su nivel educacional, la profesión, el círculo de amigos, las aficiones, etc. La información facilitada es tratada con el objetivo de elaborar un modelo adoctrinador personalizado, con el objetivo de que pueda dar solución y respuesta a todas las necesidades y preguntas existenciales presentes en el sujeto. Así es como el sujeto experimenta un mayor deseo de interactuar con los miembros de la organización y aislarse del resto de la sociedad. De esta forma, pasa a desarrollar en su psique una «sociedad paralela» (Kandel, 2004; Khosrokhaver, 2014).

En esta fase también se observa que la organización le asigna una primera tarea, que consiste en difundir y/o controlar algunas de sus páginas o redes sociales (Vicente, 2018), una tarea que el sujeto acepta al saber que actúa tras el amparo que le proporciona la pantalla y ello le proporciona confianza y seguridad.

Estas tareas acostumbran a ser delegadas a las mujeres de la organización, pues disponen de mayores habilidades sociales y comunicativas para interactuar con el futuro miembro. Una muestra de ello son las distintas detenciones de mujeres que los distintos cuerpos de seguridad del estado vienen realizando desde 2014. Reinares y García-Calvo (2017) estiman que, del total de mujeres detenidas por actividades terroristas entre 2013 a 2017, el 95,2 %

23. *The Onion Router* (TOR).
24. Estos autores identificaron siete estrategias cognitivas que permiten a los criminales contrarrestar el efecto de vínculos que normalmente impedirían cometer un delito. Estas fueron: la negación de la responsabilidad (el delincuente defiende que fue la conducta de la víctima el único responsable de su victimización); la negación del daño (el delincuente manifiesta que sus acciones no han causado ningún daño); la negación de la víctima (el delincuente justifica que la víctima se merecía el daño recibido); la condena a los condenadores (el delincuente cree que la víctima le atribuye la autoría del ilícito por actuar guiada por el despecho), y la apelación a una mayor lealtad (el delincuente alude actuar en nombre de un ser superior, para evitar un mal superior, etc).
25. Todo delito es motivado por la consecución de un beneficio. En el caso de los ciberdelitos, Turvey (2012) elaboró una clasificación con ocho motivaciones que explican el ciberdelito: *explorers, good samaritans; hackers; machiavellians; exceptions; avengers; career thieves; moles.* En el caso de las tareas de adoctrinamiento 3.0, la motivación seria la *mole*. Las personas que actúan impulsados por ella son personas que pertenecen a una organización y actúan como lo haría un «espía» en el mundo real, pues su tarea es la obtención de información para subministrarla a los miembros de la organización a la que pertenece.

de ellas tenía asignadas, entre otras, tareas dirigidas al reclutamiento y radicalización de sujetos. En caso de no haber mujeres entre sus filas, la organización se valdrá de las apariencias engañosas que internet permite elaborar y atribuir estas tareas a hombres que, tras un perfil falso de mujer, intentará convencer a otros individuos para que se sumen al terrorismo.

c) Aislamiento y adoctrinamiento: una vez la persona ha sustituido su sistema de creencias por el salafismo radical, el siguiente paso es lograr que el cambio también se generalice a su estilo de vida *offline*, pero sin que ello levante sospechas en su entorno. Para ello, la organización le autorizará a usar el *taqiyya*. Este término surge de la doctrina Takfir y se define como el acto de disimulo a través del cual se permite al creyente esconder sus propias creencias religiosas ante el temor de poder perder su vida, las vidas de sus familiares y/o para la preservación de la fe (Pérez, 2013). En la actualidad, su uso también es permitido con el fin de evitar que el creyente sea descubierto por sus intenciones terroristas y poder pasar así desapercibido en la comunidad de «infieles» para acabar sometiéndolos. De esta manera, tal como fueron testimonios las cámaras de seguridad de un club nocturno de Bruselas, pudimos ver a Salah Abdeslam (único terrorista vivo de los atentados de París de noviembre de 2015) y a su hermano, Brahim, bailando, cantando, fumando y coqueteando con chicas en una fiesta.[26] Un ejemplo más cercano en el espacio y el tiempo lo tenemos en que los responsables de los atentados de Barcelona y Cambrils nunca levantaron sospechas en su entorno próximo, sino que la percepción era que se trataba de jóvenes perfectamente integrados en la comunidad.

Los cambios conductuales que se pueden observar en esta fase son: abandono o cambio en determinadas actividades de ocio, y en caso de un individuo ya musulmán, deja de acudir a la mezquita u oratorio por considerar impura o moderada la interpretación del islam que se predica allí. También entra en conflicto con su imán y/o progenitores al considerar que no defienden al pueblo musulmán. En caso de que el sujeto sea converso, se observa que empieza a asistir a un oratorio y/o mostrar interés por la rama radical del islam y los pasajes más violentos del Corán. Esta situación se agrava si la figura paterna está ausente o no ejerce el rol del cabeza de familia. De esta manera, vemos que un cambio iniciado en el entorno *online* tiene un impacto en el entorno *offline,* corroborando así la unidad entre ambos mundos (Agustina, 2014).

d) *Jihadización*: en esta fase, el sujeto presenta un pensamiento completamente dicotomizado, así como una hipersensibilización ante cualquier conducta o comentario susceptible de ser interpretado como «ataque» contra su propia persona y/o contra la comunidad musulmana. Es en esta fase cuando se produce el primer encuentro «cara a cara» con un miembro de la organización. El encuentro tiene dos objetivos: por un lado, evaluar el nivel de fidelidad del sujeto hacia la organización y, en segundo lugar, acabar de convencerlo para que acepte las tareas que la organización le ordene, incluido el suicidio. Para ello, el adoctrinador va a potenciar las motivaciones, sentimientos y justificaciones favorables a la violencia.

Del mismo modo, en esta fase se observa a un individuo obsesionado por lograr que sus acciones trasciendan más allá de la vida terrenal. Como consecuencia del adoctrinamiento al que ha sido sometido, el sujeto ve en las acciones terroristas el medio para conseguirlo.

De acuerdo con Silber y Bhatt (2007), las tareas que la organización puede mandarle al sujeto en esta fase son: «aceptación del *jihad* y viaje a un país extranjero» (ayuda a reafirmar la decisión de llevar a cabo el *jihad* y/o de buscar la justificación religiosa que necesita previamente); «entrenamientos y preparación» (instrucción paramilitar durante la que se les enseña todo lo necesario para poner en práctica el *jihad*) y «planificación del atentado» (no solo se planificará el «cómo» se realizará el acto, sino también un plan para engendrar una nueva célula o grupo que cometa el atentado). Todas estas tareas antes requerían el desplazamiento físico del sujeto hacia un país de Oriente Próximo (Siria o Irak), pero actualmente con las TIC eso ya no es necesario, pues se pueden realizar a través del «campo de entrenamiento» virtual de la *deep web*. Ahí el sujeto tiene a su disposición revistas, comunicados, vídeos y manuales en formato multimedia que le van a enseñar cómo fabricar explosivos, utilizar armas, planificar un atentado, etc. (Cano, 2010; Cohen-Almagor, 2017).

26. Puede verse el vídeo en el siguiente enlace: <https://www.youtube.com/watch?v=-QjK85G8sMk>.

Tabla 1 Diferencia entre el proceso de adoctrinamiento en modalidad *offline* y *online*

Fase	Offline	Online
Aproximación y primeros contactos	Aproximación pasiva	Aproximación activa o pasiva
	Agente radicalizador conocido (amistad o vecindad) o familiar de la víctima	Agente radicalizador desconocido por la víctima
	Víctima de mayor edad	Víctima joven, sobre todo en período de la adolescencia
	Oratorios, mezquitas, prisión, espacios de ocio	Redes sociales
Captación, adhesión y preradicalización	Reuniones en domicilios privados	Chats privados y exclusivos que requieren de contraseña
	El grupo encarga a la víctima las primeras tareas dentro de la organización	
	Hurtos y robos	Difusión de propaganda *jihadista* en la red
Aislamiento y adoctrinamiento	Modificación del sistema de creencias, valores y estilo de vida	Modificación del sistema de creencias, valores y estilo de vida
	Uso del *Taqiyya*	
Jihadización	Campos físicos de entrenamiento Viaje a zona conflictiva	Campo de entrenamiento virtual

Elaboración propia

Conclusión

Es difícil predecir la evolución que experimentarán las organizaciones terroristas de base religiosa en los próximos años. Pero lo que sí sabemos es que su evolución irá paralela al desarrollo de las TIC.

El presente artículo ha mostrado cómo el ciberespacio se ha convertido en un medio óptimo para redefinir el delito de adoctrinamiento y radicalización *jihadista,* pudiéndose describir a través de las teorías criminológicas de la oportunidad.

En primer lugar, se ha observado que el uso de las TIC ha permitido a la organización entrar en contacto con un mayor número de «objetos apetecibles» o sujetos apropiados para ser victimizados. También hemos visto que las TIC son territorio de las nuevas generaciones y que estas se caracterizan por querer recibir rápidamente la información, realizar tareas de forma simultánea, preferir la imagen al texto y mostrar una eficacia mayor cuando trabajan en red. Esto explica por qué los jóvenes actúan con autenticidad y confianza, obviando el riesgo real que sus conductas pueden conllevar y eliminando así aquellas barreras que los pudieran proteger. Esto los convierte en un colectivo vulnerable, con alto riesgo de cibervictimización terrorista.

A diferencia de lo que sucede en el ámbito *offline*, el primer factor para que una persona pueda ser percibida como potencial víctima es que exponga previamente su intimidad e ideales en el ciberespacio. Por ejemplo, dando un «Me gusta» a una publicación del grupo Dâesh y/o colgar información que haga apología del terrorismo, reaccionar positivamente a un comentario en el que se alienta a matar a «infieles» o reenviar propaganda y colgar material que haga apología del terrorismo en su propio perfil. De forma inconsciente, el sujeto pasa de presentar un perfil de riesgo «bajo» a la victimización a uno «alto». Es entonces cuando el cibereclutador decide iniciar los primeros contactos con él. Este hecho nos permite confirmar que en el ciberespacio desaparece la necesidad de proximidad física que se requiere entre victimario y víctima en la comisión de un delito en el espacio *offline*, ya que ambos sujetos pueden converger en múltiples nodos y rutas fruto del carácter descentralizado que caracteriza a la red. A su vez, este factor hace más eficiente la comisión del delito, pues supone una disminución de costes (tanto a nivel de tiempo como de recursos) para el cibervictimario.

Otra de las características de la ciberradicalización reside en la ausencia de guardianes (o vigilantes) que puedan prevenir la victimización de un individuo. A diferencia del mundo *offline,* el anonimato que ofrece el ciberespacio hace que la perseguibilidad de los delitos se torne más complicada para los cuerpos y fuerzas de seguridad. Ello hace que la figura tradicional del «vigilante» se transforme y sea la propia víctima quien tenga que realizar sus funciones. Es decir, el sujeto debe prevenir su posible victimización reduciendo aquellas oportunidades que puedan hacer que el cibervictimario quiera iniciar contactos con él o ella. Por ejemplo, el individuo deberá dotarse de todos aquellos mecanismos de seguridad que el entorno red le ofrece, como son programas antivirus, cortafuegos, etc. No obstante, no va a ser suficiente con su instalación. La misma importancia tendrá la conducta responsable en la red que realice el individuo, realizando una estimación previa de las consecuencias que puedan tener conductas como: consultar una determinada web o colgar y/o hacer público alguna información sobre su persona. De esta manera, la víctima de ciberradicalización puede llegar a ser, en parte, corresponsable de su propia victimización. Para ello es importante educar en el uso responsable de las TIC y avisar de los peligros que uno puede encontrar en ellas. Solo a través de un uso responsable podemos minimizar el riesgo de ser victimizados.

Referencias bibliográficas

AGUSTINA, J. R. (2014). «Victimización en el ciberespacio. Victimología y victimodogmática en el uso de las TIC. Desfragmentación del yo en la era digital: 'disinhibittion effect', esquizofrenia digital e ingenuidad en el ciberespacio». En: N. PEREDA y J. M. TAMARIT (2014). *La respuesta de la victimología ante las nuevas formas de victimización*. Madrid: Edisofer.

DE LA CORTE, L. (2015). «¿Qué sabemos y qué ignoramos sobre la radicalización yihadista?». En: J. ANTON (2015). *Islamismo yihadista: radicalización y contrarradicalización*. Valencia: Tirant Lo Blanch.

BANDURA, A. (2004). «The origins and consequences of moral disengagement: A social learning perspective». En: F. M. M. MOGHADDAM, A. J. MARSELLA. (dirs.). *Understanding terrorism: Psychosocial roots, consequences and interventions.* Washington: American Psychological Association.

BAUMEISTER, R.; JONES, E. (1978). «When self-presentation is constrained by the target's knowledge: Consistency and compensation». *Journal of Personality and Social Psychology.* N.º 6, Vol. 36, pág. 608. <https://doi.org/10.1037/0022-3514.36.6.608>

BAUMEISTER, R.; LEARY, M. (2017). «The need to belong: Desire for interpersonal attachments as a fundamental human motivation». En: R. BAUMEISTER y M. LEARY *Interpersonal Development* (págs. 57-89). Londres: Routledge. <https://doi.org/10.4324/9781351153683-3>

BECOÑA, E. (2016). «Factores de riesgo y de protección en el uso problemático de Internet». En: ECHEBURÚA (Coord.). *Abuso de Internet. ¿Antesala para la adicción al juego de azar online?* Madrid: Pirámide.

BOUZAR, D. (2015). *La vie après Daesh.* París: Autrement.

BOUZAR, D. (2017). *Mon Djihad, itinéraire d'un repenti.* París: Autrement.

CANO, M. A. (2008). «Internet y terrorismo islamista. Aspectos criminológicos y legales». *Eguzkilore,* N.º 22, págs. 67-88. <http://www.ehu.eus/documents/1736829/2176658/03+Cano.indd.pdf>

CANO, M. A. (2010). *Generación Yihad. La radicalización islamista de los jóvenes musulmanes en Europa*. Madrid: Dykinson.

CARBONELL, X.; TALARN, A.; BERANUY, M.; OBERST, U.; GRANER, C. (2009). «Cuando jugar se convierte en un problema: el juego patológico y la adicción a los juegos de rol online». *Aloma*, N.º 25, págs. 201-220.

CARBONELL, X.; TORRES, A.; FUSTER, H. (2016). «El potencial adictivo de los videojuegos». En: ECHEBURÚA (Coord.). *Abuso de Internet. ¿Antesala para la adicción al juego de azar online?* Madrid: Pirámide.

COHEN-ALMAGOR, R. (2017). «Jihad Onlie: How do terrorists use the Internet?». En: R. CAMPOS, X. RÚAS, V. ALENDRO, X. LÓPEZ (2017). *Media and Metamedia Management*. Dordrecht: Springer.

COHEN, E.; FELSON, M. (1979). «Social change and crime rate trends: a routine activity approach». *American Sociological Review*. N.º 44, Vol. 44, págs. 588-608. <https://doi.org/10.2307/2094589>

CONWAY, M. (2016). «Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research». En: A. ALY, S. MACDONALD, L. JARVIS, T. CHEN. *Violent Extremism Online. New perspectives on terrorism and the Internet*. Londres: Routledge.

FELSON, M.; CLARKE, R. (1998). «Opportunity Makes the Thief. Practical theory for crime prevention». Fundación Democracia y Gobierno Local. N.º 6, págs. 193-234. Traducción disponible en: <https://www.laescenadelcrimen.com/wp-content/uploads/2017/12/laocasionhacealladron_felson_clarke.pdf>

GIDDENS, A. (2001). *Sociología*. Madrid: Alianza.

GRABOSKY, P. (2001). «Virtual criminality: Old wine in new bottles?». *Social & Legal Studies*, N.º 2, Vol. 10, págs. 243-249. <https://journals.sagepub.com/doi/10.1177/a017405#articleCitationDownloadContainer>

HOLMAN, T. (2016). «Gonna get myself connected: The role of facilitation in foreign fighter mobilizations». *Perspectives on Terrorism*. N.º 10, Vol. 2, págs. 2-23. <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/497>

JOINSON, A. (2001). «Self-disclosure in computermediated communication: the role of self-awareness and visual anonymity». *European Journal of Social Psychology,* N.º 31, págs. 77-192. <https://pdfs.semanticscholar.org/4026/45358d0b8b863060bb058b9c8b8e5cd1667e.pdf>

JORDAN, J. (2009). «Procesos de radicalización yihadista en España: Análisis sociopolítico en tres niveles». *Revista de Psicología Social*, N.º 2, Vol. 24, págs. 197-216. <https://www.ugr.es/~jjordan/publicaciones/radicalizacion.pdf>

KANDEL, J. (2004). «Organisierter Islam und gesellschaftliche Integration». *Politisceh Akademie der Friederich-Ebert-Stiftung,* págs. 1-19.

KATZ, E.; BLUMER, J.; Gurevitch, M. (1973). «Uses and Gratifications Research». *The Public Opinion Quarterly.* N.º 4, Vol. 37, págs. 509-523.

KATZ, E.; LAZARSFELD, P. (1995). *Personal Influence. The Part Played By People in The Flow of Mass Communication*. Reino Unido: Routledge.

KHOSROKHAVER, F. (2003). *Los nuevos mártires de Alá*. Madrid: Ed. Martínez Roca.

KHOSROKHAVER, F. (2014). *Radicalisation.* París: Éditions de la Maison des sciences de l'homme. <https://doi.org/10.4000/books.editionsmsh.10882>

KOZINETS, R. (2010). *Netnography: Doing Ethnographic Research Online*. Londres: SAGE.

KRUGLASKI, A.; JASKO, K.; LAFREE, G. (2016). «Quest for significance and violent extremism: the case of domestic radicalization». *Political Psychology,* N.º 5, Vol. 38.

KRUGLASKI, A.; JASKO, K.; WEBBER, D.; CNERNIKOVA, M. (2018). «The making of violent extremists». *Review of General Psychology,* N.º *22,* Vol. 1, págs. 107-120. <https://doi.org/10.1037/gpr0000144>

MCLUHAN, M.; NEVITT, B. (1972). *Take Today, the Executive as Dropout*. Estados Unidos: Harcourt Brace Jovanovich.

MIRÓ, F. (2011). «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen». *Revista Electrónica de Ciencia Penal y Criminológica,* N.º 13, págs. 1-55. <http://criminet.ugr.es/recpc/13/recpc13-07.pdf>

MIRÓ, F. (2013). «La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio». *Revista Española de Investigación Criminológica,* N.º 11, págs. 1-35. <https://dialnet.unirioja.es/servlet/articulo?codigo=4783296>

PÉREZ, O. (2013). «Takfir Wal-Hijra, entre la doctrina radical y el terrorismo yihadista». Documento de opinión 03/2013, Instituto Español de Estudios Estratégicos. <http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO03-2013_Takfir_wal-Hijra_OPVentura.pdf>

PRENSKY, M. (2001). «Digital natives, Digital immigrants». *On the Horizon*. N.º 5, Vol. 9, págs. 1-6. <https://www.emeraldinsight.com/doi/abs/10.1108/10748120110424816>

REINARES, F.; GARCÍA-CALVO, C. (2017). «Actividad yihadista en España, 2013-2017: de la Operación Cesto en Ceuta a los atentados en Cataluña». Documento de trabajo 13/2017, Real Instituto ElCano. Madrid: Real Instituto ElCano. <http://www.realinstitutoelcano.org/wps/wcm/connect/c47ba74f-38ee-4ed8-999f-8b99bd518d36/DT13-2017-Reinares-GarciaCalvo-Actividad-yihadista-en-Espana-2013-2017-Operacion-Cesto-Ceuta-atentados-Catalunya.pdf?MOD=AJPERES&CACHEID=c47ba74f-38ee-4ed8-999f-›8b99bd518d36›

REINARES, F.; GARCÍA-CALVO, C.; VICENTE, A. (2018). «Yihadismo y prisiones: un análisis del caso español». ARI 123/2018, Real Instituto ElCano. Madrid: Real Instituto El Cano. <http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari123-2018-reinares-garciacalvo-vicente-yihadismo-prisiones-analisis-caso-espanol›

SAGEMAN, M. (2004). *Understanding terror networks.* Estados Unidos: University of Pennsylvania Press.

SILBER, M.; BHATT, A. (2007). *Radicalization in the West: The Homegrown Threat.* Nueva York: Police Department.

SULER, J. (2004). «The Online Disinhibition Effect». *Cyber Psychology & Behavior.* N.º 3, Vol. 7, págs. 321-326. <https://doi.org/10.1089/1094931041291295›

SYKES, M.; MATZA, D. (1957). «Techniques of neutralization: a theory of delinquency». *American Sociologial Review*. N.º 6, Vol. 22, págs. 664-670. <https://doi.org/10.2307/2089195›

TAMIMI, A. (2007). *Hamas: A History*. Oslo: Olive Branch Press.

TOBOSO, M. (2013). «El "lobo solitario" como element emergente y evolución táctica del terrorismo yihadista». *Inteligencia y Seguridad: Revista de Análisis y Prospectiva*. N.º 14, págs. 117-150

TOFFLER, A. (1980). *La Tercera Ola*. Bogotá: Plaza & Janés Editores.

TRUJILLO, H. M.; MOYANO, M.; GONZÁLEZ-CABRERA, J. (2006). «De la agresividad a la violencia terrorista. Historia de una patología psicosocial previsible (parte II)». *Behavioral Psychology.* N.º 2, Vol. 14, págs. 289-303. <https://www.researchgate.net/publication/319902222_De_la_agresividad_a_la_violencia_terrorista_Historia_de_una_patologia_psicosocial_previsible_Parte_II›

TURVEY, B. (2012). *Criminal profiling. An introduction to behavioral evidence analysis.* Reino Unido: Elsevier.

VICENTE, A. (2018). «Fórmulas utilizadas para la radicalización y el reclutamiento yihadista de menores en España». Documento de investigación 76/2018, Real Instituto ElCano. Madrid: Real Instituto ElCano. <http://www.realinstitutoelcano.org/wps/wcm/connect/f5983a05-6ed0-41ac-9de2-652e8b972b1a/ARI76-2018-Vicente-Formulas-utilizadas-radicalizacion-reclutamiento-menores-Espana.pdf?MOD=AJPERES&CACHEID=f5983a05-6ed0-41ac-9de2-652e8b972b1a›

WALDMANN, P. (2010). «Radicalización en la diáspora: por qué musulmanes en Occidente atacan a sus países de acogida». Documento de trabajo 9/2010, Real Instituto ElCano. Madrid: Real Instituto ElCano. <http://www.realinstitutoelcano.org/wps/wcm/connect/cf7607804242a6979bb9fb8b6be8b54b/DT9-2010_Waldman_radicalizacion_diaspora_musulmanes_occidente_acogida.pdf?MOD=AJPERES&CACHEID=cf7607804242a6979bb9fb8b6be8b54b>

WALL, D. (2007). *Cybercrime: The transformation of Crime in the Information Age*. Reino Unido: Polity.

WEIMANN, G. (2004). «How modern terrorism uses the Internet». *United States Institute of Peace*. N.º 116. <https://www.usip.org/sites/default/files/sr116.pdf>

Cita recomendada

GUIRAO CID, Maria del Carme (2019). «La ciberradicalización: una nueva forma de victimización». *IDP. Revista de Internet, Derecho y Política.* N.º 29, págs. 1-19. UOC. [Fecha de consulta: dd/mm/aa]. <http://dx.doi.org/10.7238/idp.v0i29.3171>

Sobre la autora
Maria del Carme Guirao Cid
mariadelcarme.guirao@udl.cat

Universitat de Lleida
C/ de Jaume II, 73
25001 Lleida

Integradora social. Graduada en Criminología por la Universitat Oberta de Catalunya (UOC) en la mención de Seguridad y prevención. Premio extraordinario al mejor expediente de promoción. Actualmente está cursando el último curso del grado de Psicología en la misma universidad. Además, ha realizado un máster universitario en Derechos humanos, democracia y globalización (UOC) y otro en la Universidad Miguel Hernández de Valencia: Análisis y prevención del crimen.

Experta en análisis de terrorismo yihadista, insurgencias y movimientos radicales por la Universidad Pablo de Olavide de Sevilla y colaborada del Observatorio Euroasia.

Ha trabajado en el Departamento de Justicia de la Generalitat de Cataluña, concretamente en el Centro de Estudios Jurídicos y Formación Especializada (CEJFE), desde abril de 2015 a diciembre de 2017. Las tareas realizadas han consistido en dar soporte a la gestión y ejecución de planes de formación dirigidos al personal de la Administración de justicia, así como planificar, desarrollar y supervisar la implantación de las nuevas oficinas judiciales dotadas del programario informático E-Justicia.cat.

Actualmente, es investigadora predoctoral becada por la Generalitat de Cataluña, con una beca FI, en el Departamento de Derecho público de la Universitat de Lleida. Colabora con el Grup de Recerca en Victimologia i Criminalitat en la Societat de la Informació (VICRIM) del Departamento de Derecho y Ciencias Políticas de la Universitat Oberta de Catalunya (UOC).